h/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/781,284	02/13/2001	Mikio Hashimoto	203058US2RD	9450

22850 7590 11/02/2006

C. IRVIN MCCLELLAND
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SON, LINH L D	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/781,284	**Applicant(s)** MIKIO HASHIMOTO	
	Examiner Linh LD Son	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 2/06. 5/05 , DEC/04

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 07/24/06.

2. Claims 1-19 are pending.

Response to Arguments

3. Applicant's arguments filed 07/24/06 have been fully considered but they are not persuasive.

4. As per remark on page 3 2nd paragraph, Applicant argues that Eliott does not teach of the second communication path between the server and the tamper resistant processor. Examiner respectfully traverses the argument. By the broadest interpretation of the claim language, the tamper resistant processor is merely a secure tamper resistant computer (Col 10 lines 57-67). To store data for execution in a computer, a computer readable medium is well known to do just that. As in Eliot, a secure communication is set between the data storage medium and the server for transferring the encrypted program encrypted by a unique key of the tamper resistant computer or processor (Col 10 lines 57-67). Since the data is encrypted by a unique key (Col 27 lines 20-35) associating with the computer, the computer is considered to have tamper resistant feature. Therefore, Eliot is teaching claim 1.

Col 10 lines 57-67:

> (37) In this exemplary embodiment when **operating in the cartridge game play mode, serial peripheral interface 138 includes a processor (not shown) which, in addition to performing the I/O tasks referred to above, also communicates with an associated security processor 152 within storage device 54 and performs security tasks. This pair of security processors (one in the storage device 54, the other in the console 52) performs, in cooperation with main processor 100, an authentication function to ensure that only authorized storage devices may be used with video game console 52**.

Col 27 lines 20-35:

> (140) In the alternative preferred embodiment, security also is in part control led by server 101, which downloads control information to the, for example, digital signal processor associated with hard drive 206. The disk drive controller (sometimes referred to herein as a "media engine") utilizes this control information to securely control disk partitions that are created, and to control which applications have access to respective partitions. As a security measure, the insecure video game system 50 has no control over which partitions are accessible. **The disk controller's media engine responds to commands from server 101 to set up the disk partitioning. Thus, in accordance with one embodiment of the present invention, a direct security link exists between server 101 and a disk drive controller resident within the expansion device 95**. Server 101 preferably utilizes the highest degree of available Internet security features such as, for example, RSA's secure socket layer (SSL), firewalls, etc.

5. As per remark on page 4 4th paragraph, Applicant argues that Eliot does not disclose “the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key”. Similar to above interpretation, the tamper resistant computer or processor in Eliot does teach of a unique encryption key corresponding to its unique ID of the disk drive in Col 25 lines 18-28, and Col 29 lines 5-16.

> (126) Prior to explaining in detail, the presently preferred implementation, an alternative embodiment is first generally described, wherein video game system 50 is more actively involved in security operations than in the description of the preferred embodiment which follows. In accordance with this other possible exemplary embodiment, a set of **public keys are exchanged between the hard drive DSP controller 194 (FIG. 4) and server 101 (FIG. 11) under the control of the video game system processor system**. To download a game, video game system 50 sends a request to the hard drive controller 194 for a set of keys with which to encrypt. A private encryption key is then transmitted to

> server 101 in encrypted form. The server 101 encrypts the game software with the encryption key and transmits the game software for storage in hard drive 206 after processing by the video game system 50.
>
> (150) The game downloading procedure is controlled at server 101 so that only authorized games are permitted to be downloaded. **Each game is encrypted with an encryption key unique to each individual hard drive 206**. The server 101 utilizes the unique ID and encryption keys for each expansion device 95 to encrypt downloaded game software. In downloading operations, the server 101 uses a list of items for each game, including unique expansion device ID, e.g., a serial number, an expansion device 95 box encryption key and a game encryption key. In playing a game, the server 101 identifies the partitions which a particular game may access to the expansion device's disk controller.

Therefore, the rejection basis dated 02/24/06 is maintained

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-2, 4-8, 10-15, and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eliott, US Patent No. 6,468,160.

8. As per claim 1:

Eliott discloses "A program distribution device for distributing executable programs through a network to a client device having a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance" in (Col 4 lines 55-65, Col 11 lines 20-25, Col 13 lines 50-60, Col 24 lines 25-42, Col 24 lines 61-67), "the program distribution device comprising: a first communication path setup unit configured to set up a first communication path between the program distribution device and the client device for communications other than transfer of the executable programs" in (Col 26 lines 37-62); "a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor for transfer of the executable programs, the first and second communication paths being set up as different channels on an identical transmission line or as different transmission lines" in (Col 27 lines 20-48); "an encryption processing unit configured to produce an encrypted program by encrypting an executable program to be distributed to the client device" and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor" in (Col 25 lines 15-40, Col 26 lines 18-37); and "a transmission unit configured to transmit the encrypted program to the tamper resistant processor through the second communication path so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key" in (Col 25 lines 14-24, Col 25 lines 29-63, and Col 29 lines 5-17). However, Eliott does not specifically teach the tamper resistant processor. Nevertheless, Eliott does teach a computer system including: a security processor 180 to authenticate the storage device, which stores the download encrypted game, and if authenticated then the downloaded encrypted games can be accessed to for decrypting for playing (Col 25 lines 35-63). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to realize that the game system 50 is the tamper resistant processor.

9. As per claims 2, 8, and 15:

Eliott discloses "The program distribution device of Claim 1, further comprising: a user authentication unit configured to carry out authentication of a user who is using the client device, by using a user ID of the user received from the client device through the first communication path" in (Col 26 lines 55-60).

10. As per claims 4 and 10:

Eliott discloses "The program distribution device of claim 1, wherein the encryption processing unit encrypts the executable program by using the unique public key received from the tamper resistant processor through the second communication path" in (Col 27 lines 20-35).

11. As per claims 5, 11, and 18:

Eliott discloses "The program distribution device of Claim 1, wherein the encryption processing unit encrypts the executable program by using a common key, and encrypts the common key by using the unique public key received from the tamper resistant processor through the second communication path; and the transmission unit transmits the encrypted program along with an encrypted common key to the tamper resistant processor through the second communication path" in (Col 25 lines 15-27, and Col 27 lines 50-60).

12. As per claims 6, 12, and 19:

Eliott discloses "The program distribution device of Claim 1, wherein communications through the second communication path are cipher communications" in (Col 27 lines 50-55).

13. As per claims 7, and 13-14:

Eliott discloses "A client device for receiving programs distributed from a program distribution device through a network, the client device comprising: a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance" in (Col 4 lines 55-65, Col 11 lines 20-25, Col 13 lines 50-60, Col 24 lines 25-42, Col 24 lines 61-67), "a first communication path set up unit configured to set up a first communication path between the program distribution device and the client device for communications other than transfer of the executable programs" in (Col 26 lines 37-62); "a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor for transfer of the executable programs; the first and second communication paths being set up as different transmission lines" in (Col 27 lines 20-48); and a program receiving unit configured to receive an encrypted program obtained by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor, from the program distribution device through the second communication path, so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key" in (Col 25 lines 14-24, Col 25 lines 29-63, and Col 29 lines 5-17). However, Elliott does not specifically teach of encrypting the program using the unique public key, and decrypting the encrypted program using the unique secret key. Nevertheless, Elliott does discloses of encrypting the program using the private encryption key of the tamper resistant process and decrypting the encrypted program using a decryption key stored in the storage" in (Col 25 lines 14-24). The encryption key is sent to the server encrypted using the private key of the game system 50. The server receives the private encrypted encryption key and decrypts it using a prior exchanged public key of the game system 50. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify the invention to utilize only the public key of the game system 50 to encrypted the program instead of sending another encryption key to server to encrypt the program.

Further, Eliott does not specifically teach the tamper resistant processor. Nevertheless, Eliott does teach a computer system including: a security processor 180 to authenticate the storage device, which stores the download encrypted game, and if authenticated then the downloaded encrypted games can be accessed to for decrypting for playing (Col 25 lines 35-63). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to realize that the game system 50 is the tamper resistant processor.

14. As per claim 17:

Elliott does not specifically teach "the producing step encrypts the executable program by using the unique public key received from the tamper resistant processor through the second communication path". Nevertheless, Elliott does discloses of encrypting the program using the private encryption key of the tamper resistant process and decrypting the encrypted program using a decryption key stored in the storage" in (Col 25 lines 14-24). The encryption key is sent to the server encrypted using the private key of the game system 50. The server receives the private encrypted encryption key and decrypts it using a prior exchanged public key of the game system 50. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify the invention to utilize only the public key of the game system 50 to encrypted the program instead of sending another encryption key to server to encrypt the program.

15. Claims 3, 9,and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eliott, in view of Chan (Cited in PTO-892 dated 04/22/05).

16. As per claims 3, 9,and 16:

Eliott does not discloses "The program distribution device further comprising: a processor authentication unit configured to carry out authentication of the tamper resistant processor, by verifying a certificate certifying that the tamper resistant processor surely has the unique secret key and the unique public key, which is received from the client device through the second communication path". Nevertheless, Chan does discloses "The program distribution device further comprising: a processor authentication unit configured to carry out authentication of the tamper resistant processor, by verifying a certificate certifying that the tamper resistant processor surely has the unique secret key and the unique public key, which is received from the client device through the second communication path" in (Col 10 lines 4-35). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the teaching of Chan with Eliott to authenticate the game system 50 prior allow it to download any program.

17. any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2